UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,617	07/06/2001	Danny M. Nessett	3000-US-CIP	7382

56436 7590 12/26/2007

3COM CORPORATION
350 CAMPUS DRIVE
MARLBOROUGH, MA 01752-3064

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
12/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/900,617	NESSETT ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 October 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 4-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 4-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 11 October 2007.

2. Claims 1 and 4-11 are pending in the application.

3. Claims 1 and 4-11 have been rejected.

4. Claims 2, 3 and 12-72 have been cancelled.

Response to Arguments

5. Applicant's arguments with respect to claims 1-72 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1 and 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng et al U.S. Patent No. 6,418,130 B1 in view of Dole U.S. Patent No. 6,628,786 B1.

As to claim 1, Cheng et al discloses a method of re-authenticating and protecting wireless communication security [column 3, lines 44-65], comprising the steps of: a) performing a secondary authentication protocol between a wireless client electronic system (client) and a wireless network access point electronic system (AP) using a key lease generated by performance of a primary authentication protocol [column 6, lines 26-44], wherein the key lease includes a key lease period for indicating a length of time in which the key lease is valid for

using the secondary authentication protocol instead of the primary protocol [column 6, lines 26-44], and wherein the second authentication protocol includes the steps of: a(i) transmitting the key lease from the client to the AP [column 6, lines 26-44]. Cheng et al discloses transmitting the key lease from the client to the AP [column 6, lines 26-44]. Cheng et al discloses that the key lease includes an encryption key for use in the secondary authentication protocol [column 6, lines 26-44].

Cheng et al does not teach a(ii) generating a first random number associated with the client and a second random number associated with the AP, wherein the key lease includes an encryption key for use in the secondary authentication protocol. Cheng et al does not teach a(iii) transmitting the first random number to the AP and the second random number to the client. Cheng et al does not teach b) if the secondary authentication protocol is successful, generating a session encryption key for encrypting communication traffic between the client and the AP, wherein the generating comprises: b(i) applying a hash function and the encryption key to the first random number and the second random number to determine the session encryption key. Cheng et al does not teach using the encryption key, the first random number, the second random number, and a hash function to determine the session encryption key. Cheng et al does not teach applying an HMAC-MD5 algorithm and the encryption key on a concatenation of the first random number and the second random number to determine the session encryption key. Cheng et al does not teach applying a HMAC-SHA-1 algorithm and the encryption key on a concatenation of the first random number and the second random number to determine the session encryption key.

Dole teaches generating a first random number associated with the client and a second random number associated with the AP [column 6, lines 5-27]. Dole teaches transmitting the first random number to the AP and the second random number to the client [column 6, lines 5-27]. Dole teaches using the encryption key, the first random number, the second random number, and a hash function to determine the session encryption key [column 6, lines 28-36]. Dole teaches applying a HMAC-MD5 algorithm and the encryption key on a concatenation of the first random number and the second random number to determine the session encryption key [column 6 line 50 to column 7 line 2]. Dole teaches applying a HMAC-SHA-1 algorithm and the encryption key on a concatenation of the first random number and the second random number to determine the session encryption key [column 6 line 50 to column 7 line 2].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Cheng et al so that random numbers would have been generated at the client and the AP. The client's random number would have been transmitted to the AP and the AP's random number would have been transmitted to the client. The two random numbers would have been concatenated. A hashing function and an encryption key would have been applied to the concatenated random numbers. The concatenated random numbers would have been hashed with either a HMAC-MD5 or a HMAC-SHA-1 hashing function.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Cheng et al by the teaching of Dole because this method improves the quality of entropy by allowing machines with no physical source of entropy to gather entropy by communicating with other machines and insure that machines that generate

many random session keys do not run the risk of depleting their local supplies of entropy [column 4, lines 45-60].

As to claim 6, Cheng et al teaches generating a first session encryption key for encrypting communication traffic from the client to the AP [column 6 line 45 to column 7 line 6]. Cheng et al teaches generating a second session encryption key for encrypting communication traffic from the AP to the client [column 6 line 45 to column 7 line 6].

7. Claims 7-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng et al U.S. Patent No. 6,418,130 B1 and Dole U.S. Patent No. 6,628,786 B1 as applied to claim 1 above, and further in view of Kessler et al U.S. Patent No. 6,789,147 B1.

As to claims 7-11, the Cheng-Dole combination does not teach using the encryption key, the first random number, the second random number, a first media access control (MAC) address associated with the client, a second media access control (MAC) address associated with the AP, and a hash function to determine the first and second session encryption keys. The Cheng-Dole combination does not teach applying a HMAC-MD5 algorithm and the encryption key on a concatenation of the first random number, the second random number, the first media access control (MAC) address associated with the client, and the second media access control (MAC) address associated with the AP to determine the first session encryption key. The Cheng-Dole combination does not teach applying a HMAC-SHA-1 algorithm and the encryption key on a concatenation of the first random number, the second random number, the first media access control (MAC) address associated with the client, and the second media access control (MAC) address associated with the AP to determine the first session encryption key. The Cheng-Dole combination does not teach applying a HMAC-MD5 algorithm and the encryption key on a

concatenation of the first random number, the second random number, the second media access control (MAC) address associated with the AP, and the first media access control (MAC) address associated with the client to determine the second session encryption key. The Cheng et al-Dole combination does not teach applying a HMAC-SHA-1 algorithm and the encryption key on a concatenation of the first random number, the second random number, the second media access control (MAC) address associated with the AP, and the first media access control (MAC) address associated with the client to determine the second session encryption key.

Kessler et al teaches using a encryption key, a first random number, a second random number, a first media access control (MAC) address associated with the client, a second media access control (MAC) address associated with the AP, and a hash function to determine a first and second session encryption keys [column 5, lines 18-37]. Kessler et al teaches applying a HMAC-MD5 algorithm and a encryption key on a concatenation of a first random number, a second random number, a first media access control (MAC) address associated with a client, and a second media access control (MAC) address associated with a AP to determine a first session encryption key [column 7 line 54 to column 8 line 10]. Kessler et al teaches applying a HMAC-SHA-1 algorithm and a encryption key on a concatenation of a first random number, a second random number, a first media access control (MAC) address associated with a client, and a second media access control (MAC) address associated with a AP to determine a first session encryption key [column 7 line 54 to column 8 line 10]. Kessler et al teaches applying a HMAC-MD5 algorithm and a encryption key on a concatenation of a first random number, a second random number, a second media access control (MAC) address associated with a AP, and a first media access control (MAC) address associated with a client to determine a second session

encryption key [column 7 line 54 to column 8 line 10]. Kessler et al teaches applying a HMAC-SHA-1 algorithm and a encryption key on a concatenation of a first random number, a second random number, a second media access control (MAC) address associated with a AP, and a first media access control (MAC) address associated with a client to determine a second session encryption key [column 7 line 54 to column 8 line 10].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Cheng-Dole combination so that a encryption key, a first random number, a second random number, a first media access control (MAC) address associated with the client, a second media access control (MAC) address associated with the AP, and a hash function would have been used to determine a first and second session encryption keys. The first session encryption key would have been determined by applying either a HMAC-MD5 or HMAC-SHA-1 hashing function and a encryption key to the concatenation of a first random number, a second random number, a first media access control (MAC) address associated with a client, and a second media access control (MAC) address associated with a AP. The second session encryption key would have been determined by applying either a HMAC-MD5 or HMAC-SHA-1 hashing function and a encryption key to the concatenation of a first random number, a second random number, a first media access control (MAC) address associated with a client, and a second media access control (MAC) address associated with a AP.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Cheng-Dole combination by the teaching of Kessler et al because it provides a system that does not require a large amount of resources to be consumed

with establishing secure sessions and it reduces latency and provides enhanced security [column 2, lines 27-39].

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy AM
December 20, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100